PATENT APPLICATION
SS-747-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Your petitioners, Bertrand TEPLITXKY, a citizen of the United States and a resident of California, whose post office address is 10385 Farallone Drive, Cupertino, CA 95014; and, Lawrence G. MARTINELLI, a citizen of the United States and a resident of California, whose post office address is 5052 Woodland Drive, Placerville, CA 95667, prays that letters patent may be granted to them for a

SECURE PRODUCT PACKAGING SYSTEM

as set forth in the following specification.

SECURE PRODUCT PACKAGING SYSTEM

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to product packaging, and in particular to secure packaging and sealing systems that combat tampering, gray marketing, and product counterfeiting.

Description of the Prior Art

The general public is now very familiar with product packages and seals that are used to make product tampering obvious to the consumer. These measures developed in part from past cases of food and medicine tampering that ended in a few cases of poisoning and a public panic. One case in particular, the Tylenol pain-reliever tainting with cyanide, is infamous.

Some foods spoil more quickly once the bottle or package has been entered. So many producers include devices and labels that warn a consumer if the package has been opened. For example, foods in glass jars are sealed by their tops under vacuum. When the lid is opened, the vacuum is lost and the metal lid top bubbles up and no longer down. A warning label warns consumers to look for this condition to ensure product freshness and safety.

Product counterfeiting presents a very different situation for both consumers and producers. Some products have such high price points that it makes it very affordable for a counterfeiter to exactly duplicate

all the packaging, and its associated seals and security devices. For example, common prescriptions now retail for $10-20 a pill. Some cancer medicines can retail for over $10,000 for a 30-day supply for one user. Any and all safety and security measures can be duplicated and impersonated by counterfeit products that don't have to bear the development and marketing costs. Many commercial manufacturers suffer large losses to counterfeiters, and so they often are subjected to financial reserves that can approach 50% of their gross sales.

SUMMARY OF THE INVENTION

Briefly, a product security system embodiment of the present invention includes an RFID chip and antenna that are polymerized onto separable parts of a commercial product package. The RFID chip includes a unique serial number that can be interrogated by a wireless reader. A database of such unique serial numbers associated with particular manufacturing production runs is used in a method to detect counterfeiting. The RFID chip and antenna are embedded such that attempts to remove or transfer them will be obvious to an inspector.

An advantage of the present invention is that a system is provided for detecting product tampering.

Another advantage of the present invention is that a method is provided for detecting product counterfeiting.

A further advantage of the present invention is that retro-fit security system is provided for existing products.

These and other objects and advantages of the present invention will no doubt become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

IN THE DRAWINGS

Fig. 1 is a functional block diagram of a product security system embodiment of the present invention;

Fig. 2 is a flowchart diagram of a method embodiment of the present invention;

Fig. 3A is a plan view of a security device embodiment of the present invention for a bottle or jar with a simple cap;

Fig. 3B is a perspective view of the security device of Fig. 3A embedded in the cap of a jar and showing the tabs that are to be wrapped and permanently bonded to the body of the jar;

Fig. 4A is a plan view of a security device embodiment of the present invention for a bottle or jar with a security cap that breaks apart when twisted open by a user; and

Fig. 4B is a perspective view of the security device of Fig. 4A, with its antenna embedded in the top part of a security cap of a jar, and showing the RFID chip embedded in the bottom lower ring part of the security cap.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Fig. 1 represents a product security system embodiment of the present invention, and is referred to herein by the general reference numeral 100. The product security system 100 comprises a portable tag reader 102 for inspecting a commercial packaged product 104. The reader 102 will assist a user in determining if there has been any tampering or counterfeiting of the product 104. A lid 106 screws onto a matching jar 108 filled with a product 110.

A radio frequency identification (RFID) chip 112 is connected to a tuned antenna 114, e.g., operating at 13.56 MHz. A thermosetting cross-linked polymer 116 "plastic-welds" the antenna to the lid 106. Similarly, another thermosetting cross-linked polymer 118 plastic-welds the RFID chip 112 to the jar 108.

A pre-tear 120 favors ripping the antenna 114 at the container separation line when the consumer opens or otherwise penetrates the packaged product 104. When the product is accessed, the antenna 114 will be damaged, and any electronic access to the RFID chip 112 will be impossible.

In alternative embodiments of the present invention, a sensor 122 is included to monitor a physical characteristic of the container product 110. For example, the sensor 122 can be configured to measure the density, composition, chemistry, pH, electrical resistance, color, turbidity, volume, vapor pressure, viscosity, reactive fluorescence, etc. A calibrated

digital or analog measurement is not strictly necessary, it is only important for the RFID chip 112 to be able to report any significant change in such physical characteristic of the container product 110 since being sealed. Such changes can be interpreted to indicate product tampering, spoiling, and counterfeiting.

A radio link 124 is established when the reader 102 is activated and brought close enough to the antenna 114. In general, this distance will be a few inches, and that is important to guarantee an intimate communication link not interfered with by other devices. It can therefore be important to place the antennas 114 on the tops of packages 104 if they are to be shipped together in multiple unit boxes. A reader 102 can be passed over the top of such a shipping box to interrogate each and every package 104 inside.

The portable tag reader 102 comprises an antenna 126, an RFID reader 128, a database 130, and a user display 132. Commercial devices being marketed that can be used for RFID chip 112 and RFID reader are available from Atmel Corporation (San Jose, CA) as RFID "transponders" and "read/write base stations". Other such devices and operating frequencies can be used. An important aspect of any device selected for use is that it have a unique serial number and that wireless access cannot occur if its antenna is damaged.

The "plastic-welding" mentioned is accomplished in original production by vulcanizing constituent monomers with heat into long-chain cross-linked polymers that respectively entangle the RFID chip 112 and antenna 114. Any attempts to remove the RFID chip 112 and antenna 114 will be easily spotted and detected, because the bonding cannot be reconstituted or effectively substituted.

The RFID chip 112 includes a unique serial number that can be read-out by the reader 102 under certain conditions. If the unique serial number cannot be read out, then the container product 110 is assumed to be tainted or counterfeit. If the unique serial number can be read, it is used to see if it matches an original product production series number maintained by the legitimate manufacturer of the product 110.

The RFID chip 112 requires that the reader 102 be close enough to induce operating power to respond in its antenna 114. Such must be properly tuned and not broken in order to capture sufficient energy to power the RFID chip 112.

The reader 102 will assist a user in determining if there has been any tampering or counterfeiting of the product 110.

As described by Atmel Corporation, radio frequency identification (RFID) involves contactless reading and writing of data into an RFID tag's nonvolatile memory through an RF signal. An RFID system typically consists of an RFID reader and an RFID tag. The reader emits an RF signal, and data is exchanged when the tag comes close to the reader signal. The Atmel RFID tags derive their operating power from the RF reader signal, so a battery or external power source is not needed. Atmel Corporation markets a line of contactless RFID integrated circuits chip IC's, micromodules, and transponders operating at 125 kHz and 13.56 MHz. For contactless smart card applications, Atmel markets a line of 13.56 MHz Secure RF Smart Card ICs based on EEPROM technology. A new CryptoRF™ family is available with low cost, secure RF memory devices that share identical cryptographic algorithms and security features. Security

is provided by encrypted passwords, mutual authentication, data encryption and encrypted checksums. CryptoRF devices are available with user memories of 1-64 kilobits of EEPROM. The CryptoRF devices are compliant with the ISO/IEC 14443 Type B standards. A contactless smart card system includes an RF reader and an RF card. The reader emits an RF signal which polls for cards. Data is exchanged when the card is within the RF field of the reader antenna.

In reference to cross-linked polymers 116 and 118 (Fig. 1), polymers in general comprise repeating molecules. These repeating molecules tend to form long chains that get tangled together. For example, polyolefins (waxes), polyacrylates (acrylics), polysulfides, polyvinylchlorides (PVC), polytetrafluoroethylene (PTFE or Teflon), and polyurethanes.

Polymerization is the process of joining together the component molecules of the polymer. In the rubber industry, polymerization is known as "vulcanization". In the fiberglass industry, polymerization is referred to as the "cure".

Polymers may be realized in a variety of viscosities, such as an oil (liquid), a gum (thixotropic gel), and a rubber (solid). An oil is made of short loosely-tangled pieces of "thread", a rubber is made up of long tightly-knotted tangles of "thread". The tangling of the "threads" of a polymer is called cross-linking and the process of tangling is called polymerization. Cross-linking and polymerization are what happens when portions of the polymer chains interact with each other.

A "fully polymerized" polymer is not usually dissolved in a solvent, the tangled knots can't be untied. Breaking the polymer down into its individual component molecules loses the road-map or guide to the organization of the component parts, and cannot be put back together into the polymer.

Some polymers have tight rigid bonds with highly organized chains, like polymethacrylates (acrylics) which are hard but brittle. Other polymers have loose and flexible bonds, like silicone rubber which is resilient and elastic

A particular silicone polymer may be in various physical states which is usually determined by the length of the polymer chains and the degree of cross-linking between these chains. A fluid (silicone oil) has short polymer chains with limited cross-linking between chains (short loosely tangled threads). Gums have longer polymer chains and a greater degree of cross-linking (longer and more tightly knotted chains). Rubbers have long chains that are highly organized and cross-linked.

The manufacture of conventional silicone rubber involves extensive cross-linking between chains of a polymer. As the reaction proceeds, the reactive sites on each chain react other reactive sites, forming a highly cross-linked network of polymer. Silicone rubber is made by letting this cross-linking reaction proceed until all the reactive sites are linked.

Fig. 2 illustrates a method embodiment of the present invention for product security, and is referred to herein by the general reference numeral 200. The method 200 comprises packaging products that have unique serial numbers that can be wirelessly interrogated, as in a step 202. A manifest 204 of original production series

numbers is built from the unique product serial numbers and maintained in a manufacturer database 206. At the factory, a check 208 is made to see if the wireless reading of the product unique serial number can be done, and that it matches what is expected from the database 206. If not, a problem is detected and an investigation is made in a step 210. Otherwise, the product 214 can be shipped to the wholesale level.

At wholesale, the product 214 may not be the product 202 that the manufacturer produced, e.g., it has been counterfeited. A wholesaler's database 212 is derived by trusted channels from the manufacturer's database 206. A check of the numbers in a step 216 will detect a counterfeit product that otherwise looks perfect. If the correct numbers are returned by a reader, then the product proceeds to the retail level as a product 220.

Again, the product 220 may have been counterfeited or tampered with, and a retailer's database 218 is used in a step 222 to detect a problem. If the product numbers check, then the product is made available to the consumer level. Such retailer's database 218 can be copied from an appropriate part of wholesaler's database 212 or manufacturer database 206. The Internet can be used to securely communicate these databases.

A user inspection 224 is mostly visual, e.g., referring to Fig. 1, looking at the embedding of the tuned antenna 114 in the cross linked polymer 116 and the RFID chip 112 in cross linked polymer 118. If not intact, the consumer is advised to discard the product and investigation 210 should be conducted. Otherwise, the product is assumed to be pristine and legitimate and can be used with confidence.

Alternative embodiments of the present invention incorporate the same pieces of Fig. 1 in different ways to suit a variety of product packages. For example, plastic jars, pill bottles, aluminized pouches, blister packs, wine bottles, boxes, security badges, identification cards, passports, etc. The system 100 can be retrofitted and permanently "glued" to an existing packaging. For new package designs, the electronic components can be embedded or encapsulated in the very fabric of the packaging material.

Fig. 3A represents a security device embodiment of the present invention for a bottle or jar with a simple cap, and is referred to herein by the general reference numeral 300. In Fig. 3B, security device 300 is shown partially embedded in a cap 302 of a jar 304. A pair of tabs 306 and 307 are to be wrapped and permanently bonded to the body of the jar. An RFID chip 308 is included between tabs 306 and 307 and will separate from an antenna 310 if any stress is applied to a notch 312. During product manufacturing and packaging, the cap 302 is twisted onto jar 304 and tabs 306 and 307 are bonded to the neck of jar 304. Twisting off the cap 302 will break the antenna 310 and prevent functioning of RFID chip 308. Before any opening or tampering, the RFID chip 308 can be interrogated through antenna 310 to report its unique serial number to a wireless reader.

Fig. 4A represents another security device embodiment of the present invention for a bottle or jar with a security cap, and is referred to herein by the general reference numeral 400. In Fig. 4B, security device 400 is shown embedded between a security-cap top 402 and a break-away ring 403. The cap is screwed onto a jar 404 during product packaging and ring 403 will remain

thereafter on jar 404. A bottom substrate 406 supports an RFID chip 408 and are embedded in ring 403. RFID chip 408 is electrically connected to an antenna 410 that will separate at a notched area 412 if enough stress is applied. Normally, twisting off the cap 402 will break the antenna 410 and thus prevent functioning of RFID chip 408. Before any opening or tampering, the RFID chip 408 can be interrogated through antenna 410 to report its unique serial number to a wireless reader.

Although the present invention has been described in terms of the presently preferred embodiments, it is to be understood that the disclosure is not to be interpreted as limiting. Various alterations and modifications will no doubt become apparent to those skilled in the art after having read the above disclosure. Accordingly, it is intended that the appended claims be interpreted as covering all alterations and modifications as fall within the "true" spirit and scope of the invention.

What is claimed is: